IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Patent Application of	Confirmation No.: 1503
MUDHAR	Atty. Ref.: 36-2021
Serial No. 10/593,588	TC/A.U.: 2617
Filed: September 21, 2006	Examiner: K. Wang-Hurst
For: ADAPTIVE CLOSED GROUP CARICATURING	

* *

June 10, 2009

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

Sir:

Appellant hereby appeals to the Board of Patent Appeals and Interferences from the last decision of the Examiner.

TABLE OF CONTENTS

(I)   REAL PARTY IN INTEREST

The real party in interest is British Telecommunications public limited company, a corporation of the country of the United Kingdom.

1490183

(II)   <u>RELATED APPEALS AND INTERFERENCES</u>

The appellant, the undersigned, and the assignee are not aware of any related

appeals, interferences, or judicial proceedings (past or present), which will directly affect

or be directly affected by or have a bearing on the Board's decision in this appeal.

1490183

(III)   STATUS OF CLAIMS

Claims 1-16 are pending and have been rejected. No claims have been substantively allowed. All of rejected claims 1-16 are being appealed.

1490183

(IV)   STATUS OF AMENDMENTS

A Response requesting reconsideration of the Final Rejection was filed on March 9, 2009. An Advisory Action was issued on March 24, 2009 continuing to reject all claims.

1490183

(V)   SUMMARY OF CLAIMED SUBJECT MATTER

Each independent claim, each dependent claim argued separately, and each claim having means plus function language is summarized below including exemplary reference(s) to page and line number(s) of the specification.

1.   A method of authorising data transfer to or from a mobile node temporarily connected to an attachment point of a network, the attachment point having a forwarding node associated therewith for forwarding messages to or from the mobile node, the method including the steps of:

(a)   receiving a digital certificate from the forwarding node, which certificate includes a message body and a digital signature for verifying the content of the message body, the message body having geographical information therein, which geographical information is derived from a physical location [Fig. 2, ref. no.s 50-58; page 5, lines 23-30];

(b)   performing a comparison between the geographical information of the certificate and other information [page 6, lines 26-32]; and,

(c)   making an authorisation decision for data transfer to or from the mobile node in dependence on the result of the comparison [page 6, line 32 to page 7, line 16].

13.   A network node for authorising the transfer of data to a mobile node temporarily connected to a forwarding node, wherein the network node is configured, in response to receiving a digital certificate from the forwarding node,

to read at least part of the digital certificate, the digital certificate including

geographical information derived from a physical location [Fig. 2, ref. no.s 50-58;

page 5, lines 23-30], and wherein the network node is further configured to:

perform a comparison between the geographical information of the certificate and

other information [page 6, lines 26-32]; and, in dependence on the result of the

comparison, make an authorisation decision [page 6, line 32 to page 7, line 16].

14.   A method of authorising data transfer to or from a mobile node

using a digital certificate, wherein the digital certificate includes a message body,

a digital signature for verifying the content of the message body, the message

body having geographical information derived from a physical location [Fig. 2, ref.

no.s 50-58; page 5, lines 23-30], the method including the steps of: receiving the

digital certificate from the mobile node; performing a comparison between the

geographical information of the certificate and other information [page 6, lines 26-

32]; and, making an authorisation decision in dependence on the result of the

comparison [page 6, line 32 to page 7, line 16].

(VI) GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

A. Claims 1-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stewart in view of Sharma et al.

B. Claims 13-16 are rejected under 35 U.S.C. 102(a) as being anticipated by Stewart.

1490183

(VII)   ARGUMENT

A.   Claims 1-12 are not obvious under 35 U.S.C. 103(a) in view of Stewart and Sharma.

The Examiner alleges that Stewart discloses a digital certificate . . . which certificate includes a message body . . . the message body having geographic information therein." *See,* Final Office Action at page 4. For support of this allegation the Examiner cites to Stewart:

> Billing for access to the network communication service, i.e., the amount the "value bucket" is drained or filled, may be based on one or more of a number of factors, including information stored in the digital certificate, such as sponsorship information, the geographic location of the user, demographic information of the user, and charging information of the user. As noted above, geographic location information of the MU may be provided to the network through the AP. This geographic location information may thus be used, in addition to other information, to adjust the billing rate or amount for network access.

See, for example, Stewart at column 3, lines 33-44 and the Abstract. However, the cited portion of Stewart does not actually state that the geographical information is contained in the digital certificate. The Examiner has construed the term "such as" in the cited passage to refer to the "sponsorship information" as well as the subsequently mentioned "geographical location of the user", the "demographic information" and "charging information of the user." This is clearly an error as will be explained in detail below.

- 10 -

1490183

It is respectfully submitted that the cited passage, when viewed in the context of the document as a whole, is properly interpreted such that only the sponsorship information is specified as being in the certificate, the remaining types of information each simply being one of the "one or more factors" referred to in the passage. Furthermore, from the context of the document as a whole, it is respectfully submitted that it is in fact clear that the geographical information is outside the digital certificate and that any other interpretation is nonsensical.

This is established by considering the passage at column 1, line 55, which states that digital certificates store non-changeable information, and that the contents of the certificate are determined to be valid and-modified. Moreover, as is clear from the passage beginning at column 2, line 30, the user is a mobile user whose geographical location changes. Clearly, Stewart's geographical information cannot be in the certificate, since the geographical information changes whereas the certificate is said to contain non-changing information. Furthermore, there is no mention of a procedure for incorporating changed information into the certificate in a secure manner, which a person skilled in the art would understand to be necessary if the geographical information where to be incorporated into the certificate each time the geographical location of a user changed.

In addition, it is stated on numerous occasions in the text, such as at column 2, line 55, column 5, line 55, and even in the Examiner's cited passage at

- 11 -

1490183

column 3, line 40, <u>that the access points (APs) provide the geographical</u>

<u>information, whereas the digital certificate is installed on the client computer</u>.

Clearly, the geographical information provided by the access points <u>cannot be in</u>

<u>a digital certificate if the digital certificate is on the client computer</u>. In any event,

there appears to be no reason for the geographical information to be transmitted

in the digital certificate from a client computer, <u>since it is already transmitted by</u>

<u>the access point</u>.

Returning to the detailed description of the Stewart embodiments, the

passage at column 9, lines 35-58 describes in detail how the digital certificate is

used. Again, it is clear that sponsorship information is in the digital certificate,

but there is <u>no mention of geographical information</u>. In addition, at column 12,

lines 33-38, it is made clear that the digital certificate can contain a reference to a

database which stores information that changes frequently, whereas the digital

certificate itself stores information that changes less frequently. Clearly, it follows

that Stewart's geographical information is stored in the database rather than the

digital certificate, since the geographical information changes frequently for

mobile users. Indeed, it is noted that there is simply no mention or suggestion in

Stewart that the geographical information is static.

Since Stewart makes no mention or suggestion of providing geographical

information in a digital certificate, it is not believed necessary to discuss Sharma

which has been cited only for "teaching a forwarding node." *See,* Office Action at

- 12 -

page 4. Accordingly, claims 1-12 patentably define over the cited art, taken singly or in combination, for the reasons given above.

B. Claims 13-16 are not anticipated under 35 U.S.C. 102 in view of Stewart.

For the same reasons given above with respect to the rejection of claims 1-12, claims 13-16 patentably define over Stewart. Stewart makes no mention or suggestion of providing geographical information in a digital certificate and, therefore, Stewart cannot anticipate claims 13-16 which clearly require this feature.
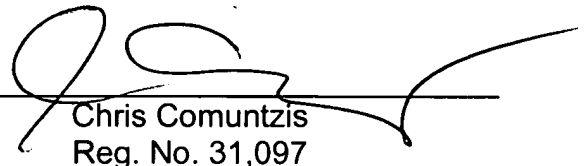
CONCLUSION

In conclusion it is believed that the application is in clear condition for allowance; therefore, early reversal of the Final Rejection and passage of the subject application to issue are earnestly solicited.

Respectfully submitted,

NIXON & VANDERHYE P.C.

By: _____
Chris Comuntzis
Reg. No. 31,097

CC:lmr
901 North Glebe Road, 11th Floor
Arlington, VA 22203-1808
Telephone: (703) 816-4000
Facsimile: (703) 816-4100

1490183

(VIII) CLAIMS APPENDIX

1.   A method of authorising data transfer to or from a mobile node

temporarily connected to an attachment point of a network, the attachment point

having a forwarding node associated therewith for forwarding messages to or

from the mobile node, the method including the steps of:

(a)   receiving a digital certificate from the forwarding node, which

certificate includes a message body and a digital signature for verifying the

content of the message body, the message body having geographical

information therein, which geographical information is derived from a physical

location;

(b)   performing a comparison between the geographical information of

the certificate and other information; and,

(c)   making an authorisation decision for data transfer to or from the

mobile node in dependence on the result of the comparison.

2.   A method as claimed in claim 1, wherein the digital certificate is

suitable for use in a public key encryption system.

3.   A method as claimed in claim 2, wherein the certificate is generated

at a certificating node having a public key and a private key associated therewith,

and wherein the signature is a function, at least in part, of the private key of the

certificate node.

1490183

4.   A method as claimed in claim 2, including the step of verifying the authenticity of the digital certificate by performing a computation on at least part of certificate, the computation involving the public key associated with the certificate node.

5.   A method as claimed in claim 1, wherein the mobile node has a certificate associated therewith, which certificate includes geographical information, the method including the further step of receiving the certificate from the mobile node, and using the geographical information from the certificate of the mobile node to make the authorisation decision.

6.   A method as claimed in claim 1, wherein a registration procedure is performed to allow data transfer between the forwarding node and the mobile node, and wherein the registration procedure includes the steps of: receiving, at the forwarding node, a certificate with geographical information therein; and, comparing the received geographical information with other information.

7.   A method as claimed in claim 1, wherein the geographical information in the certificate associated with the forwarding node is derived from the physical location of the forwarding node.

8.   A method as claimed in claim 1, wherein the mobile node has a temporary address and a permanent address associated therewith.

9.   A method as claimed in claim 8, wherein the temporary address of the mobile node is indicative of the topological position of the current point of attachment of the mobile node.

10.   A method as claimed in claim 8, including the steps of: (i) intercepting packets addressed to the permanent address of the mobile node; and, (ii) forwarding the intercepted packets towards the temporary address of mobile node, at least one of steps (i) and (ii) being authorised in dependence on the result of a comparison involving geographic information within a certificate.

11.   A method as claimed in claim 1, wherein the forwarding node is a fixed node.

12.   A method as claimed in claim 1, including an authentication step.

13.   A network node for authorising the transfer of data to a mobile node temporarily connected to a forwarding node, wherein the network node is configured, in response to receiving a digital certificate from the forwarding node, to read at least part of the digital certificate, the digital certificate including geographical information derived from a physical location, and wherein the

- 16 -

1490183

network node is further configured to: perform a comparison between the geographical information of the certificate and other information; and, in dependence on the result of the comparison, make an authorisation decision.

14.   A method of authorising data transfer to or from a mobile node using a digital certificate, wherein the digital certificate includes a message body, a digital signature for verifying the content of the message body, the message body having geographical information derived from a physical location, the method including the steps of: receiving the digital certificate from the mobile node; performing a comparison between the geographical information of the certificate and other information; and, making an authorisation decision in dependence on the result of the comparison.

15.   A method as claimed in claim 14, wherein the mobile node is configured to form a temporary attachment to an attachment point of a main network, and wherein the digital certificate is received at a network node in the main network.

16.   A method as claimed in claim 15, wherein the attachment point has a forwarding node associated therewith for forwarding messages to and/or from the mobile node, and wherein the forwarding node has a digital certificate associated therewith, which certificate include geographical information derived from the physical location of the forwarding node, the method including the steps

- 17 -

of: at the network node, receiving the digital certificate from the forwarding node;

and, making an authorisation decision in dependence on the geographical

information of the certificate from the forwarding node.

1490183

(IX)   **EVIDENCE APPENDIX**

None.

1490183

(X)   <u>RELATED PROCEEDINGS APPENDIX</u>

None.